ประกาศการประปานครหลวง
เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

โดยที่เป็นการสมควรปรับปรุงนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) และกำหนดแนวทางการบริหารจัดการข้อมูลของการประปานครหลวงให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล ลงวันที่ ๒๔ กรกฎาคม ๒๕๖๖ เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ ตลอดจนกฎหมาย กฎระเบียบ และข้อกำหนดอื่นที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๓๑ มาตรา ๓๒ และมาตรา ๓๓ (๒) แห่งพระราชบัญญัติการประปานครหลวง พ.ศ. ๒๕๑๐ ผู้ว่าการการประปานครหลวงจึงให้ยกเลิกประกาศการประปานครหลวง เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ลงวันที่ ๑๕ กันยายน พ.ศ. ๒๕๖๖ และกำหนดนโยบายดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศการประปานครหลวง เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"การกำกับดูแลข้อมูล (Data Governance)" หมายถึง การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์ การตัดสินใจเชิงนโยบาย และการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปขอเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"องค์กร" หมายถึง การประปานครหลวง

"มาตรฐาน" หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

"แนวปฏิบัติ" หมายถึง แนวทางที่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมาย

คำอธิบาย...

"คำอธิบายข้อมูล (Metadata)" หมายถึง ข้อมูลที่ใช้อธิบายชุดข้อมูล โดยระบุรายละเอียดแหล่งข้อมูลและคำอธิบายรายละเอียดเกี่ยวกับข้อมูล

"ชุดข้อมูล (Dataset)" หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

"การบริหารจัดการข้อมูล (Data Management)" หมายถึง ขั้นตอน วิธีการ หรือกระบวนการใด ๆ อันนำไปสู่การสร้างข้อมูล รวมรวบข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

"บัญชีข้อมูล (Data Catalog)" หมายถึง เอกสารแสดงรายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มจัดประเภทชุดข้อมูลที่อยู่ในการครอบครองหรือการควบคุมของการประปานครหลวง

"ข้อมูลหลัก (Master Data)" หมายถึง ข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลผู้ใช้น้ำ ข้อมูลน้ำดิบ ข้อมูลคุณภาพน้ำประปา เป็นต้น โดยข้อมูลที่ถูกสร้างจากหน่วยงานหรือระบบต้นทาง หรือข้อมูลที่ถูกจัดเก็บไว้แหล่งเดียว มีการกำหนดมาตรฐานของข้อมูล เพื่อช่วยลดความซ้ำซ้อนของข้อมูล เพื่อให้ข้อมูลมีคุณภาพ

"ข้อมูลสำคัญ (Critical Data Element)" หมายถึง ข้อมูลที่มีความสำคัญและได้มาจากกระบวนการทางธุรกิจ อาจเป็นข้อมูลหลักที่สร้างขึ้นเพื่อใช้งานในองค์กรหรือถูกใช้ในรายงานทางธุรกิจระดับสูงขององค์กร

"ชุดข้อมูลที่มีคุณค่าสูง (High Value Datasets)" หมายถึง ชุดข้อมูลที่มีประโยชน์ต่อหน่วยงานของรัฐและผู้ใช้ข้อมูล โดยเป็นข้อมูลที่ตรงตามความต้องการของผู้ใช้ข้อมูลอย่างแท้จริง และสามารถนำไปใช้ต่อได้อย่างกว้างขวาง

"คณะกรรมการ" หมายถึง คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของการประปานครหลวง

"ผู้มีส่วนได้ส่วนเสียกับข้อมูล" หมายถึง หน่วยงานหรือกลุ่มคนที่สร้างข้อมูล หรือใช้ข้อมูล

"เจ้าของข้อมูล (Data Owner)" หมายถึง หน่วยงานที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

"หัวหน้าบริกรข้อมูล (Lead Data Steward)" หมายถึง คณะทำงานที่ทำหน้าที่เป็นผู้ควบคุมและสั่งการทีมบริกรข้อมูล รวมทั้งเป็นหนึ่งในคณะกรรมการธรรมาภิบาลข้อมูล

"บริกรข้อมูล (Data Steward)" หมายถึง บริกรข้อมูลเชิงธุรกิจ บริกรข้อมูลเชิงเทคนิค ทำหน้าที่นิยามคำอธิบายข้อมูลหรือมาตรฐานข้อมูล หรือกำหนดนโยบายเกี่ยวกับข้อมูล และอาจรวมไปถึงกำหนดเกณฑ์คุณภาพข้อมูลด้วย

ข้อ ๔ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มีดังต่อไปนี้

๔.๑ ขอบเขตนโยบายธรรมาภิบาลข้อมูล มีดังต่อไปนี้

๔.๑.๑ กำหนดให้มีการจัดตั้งคณะกรรมการ โดยคณะกรรมการต้องประกอบไปด้วยผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บริหารจากส่วนงานต่าง ๆ ที่เกี่ยวข้อง และหัวหน้าบริกรข้อมูล โดยให้เลขานุการคณะกรรมการปฏิบัติหน้าที่หัวหน้าบริกรข้อมูลด้วยอีกหน้าที่หนึ่ง

๔.๑.๒ กำหนดหน่วยงานที่เป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลในแต่ละชุดข้อมูล

๔.๑.๓ ให้มีการกำหนดข้อมูลหลัก (Master data) รวมถึงข้อมูลสำคัญ (Critical Data Element) และชุดข้อมูลที่มีคุณค่าสูง (High-value dataset)

๔.๑.๔ จัดทำนโยบาย...

๔.๑.๔ จัดทำนโยบายธรรมาภิบาลข้อมูลที่ประกอบไปด้วย นโยบายการบริหารจัดการวงจรชีวิตข้อมูล (Data Lifecycle Management Policy) นโยบายการบริหารจัดการคำอธิบายข้อมูล (Metadata Management Policy) นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการจัดหมวดหมู่และชั้นความลับข้อมูล (Data Categories and Classification Policy) นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Exchange Policy) นโยบายการเปิดเผยข้อมูล (Open Data Policy) และนโยบายความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูล (Data Security and Privacy Policy)

๔.๑.๕ กำหนดให้ธรรมาภิบาลข้อมูลครอบคลุมตลอดวงจรชีวิตข้อมูล (Data Life Cycle) ตั้งแต่กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการประมวลผลและการใช้ข้อมูล (Process and Use) กระบวนการเปิดเผยและการรักษาความลับข้อมูล (Disclosure and Confidentiality) กระบวนการจัดเก็บข้อมูลถาวร (Achive) กระบวนการทำลายข้อมูล (Destroy)

๔.๑.๖ ให้กำหนดกระบวนการธรรมาภิบาลข้อมูลอย่างเป็นรูปธรรม

๔.๑.๗ ให้มีการสื่อสารและเผยแพร่นโยบายธรรมาภิบาลข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน

๔.๑.๘ ให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการและวงจรชีวิตของข้อมูล

๔.๒ องค์ประกอบของนโยบายธรรมาภิบาลข้อมูล มีดังต่อไปนี้

๔.๒.๑ นโยบายการบริหารจัดการวงจรชีวิตข้อมูล

๑) กระบวนการสร้างข้อมูล (Create)

(๑) ให้มีการกำหนดสิทธิการเข้าถึงข้อมูล วิธี และเครื่องมือที่ใช้ในการสร้างข้อมูล โดยมีข้อกำหนดที่ชัดเจน ตามมาตรฐานให้เป็นแบบเดียวกัน

(๒) กำหนดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลต่าง ๆ ได้อย่างเหมาะสม รวมถึงการสร้างจิตสำนึกในการรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยข้อมูล

(๓) กำหนดสร้างความรู้ความเข้าใจในการสร้างข้อมูลแก่ผู้ที่เกี่ยวข้อง

๒) กระบวนการจัดเก็บข้อมูล (Store)

(๑) ให้มีการกำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และจัดเก็บลงในสื่อบันทึกข้อมูล ตามมาตรฐานสถาปัตยกรรมข้อมูล ซึ่งเป็นที่ยอมรับในระดับสากล

(๒) ให้มีการร่วมกันกำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย ความเป็นส่วนบุคคล และคุณภาพข้อมูล

(๓) ให้มีการสร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้อง รวมถึงแจ้งให้ผู้มีส่วนได้ส่วนเสียภายนอกถึงเหตุผลในการจัดเก็บข้อมูล

(๔) ให้มีการจัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน

(๕) ให้มีการร่วมกันจัดให้มีกระบวนการทดสอบข้อมูลที่จัดเก็บว่ามีคุณภาพตามเกณฑ์คุณภาพข้อมูล

(๖) ให้มีการกำหนดหมวดหมู่และระดับชั้นความลับข้อมูล โดยให้เป็นไปตามนโยบายการจัดหมวดหมู่และระดับชั้นความลับข้อมูล หรือตามที่กฎหมายกำหนด

(๗) มีการสำรองข้อมูลหากเกิดเหตุฉุกเฉิน โดยข้อมูลจะต้องสามารถใช้งานได้อย่างต่อเนื่อง

๓) กระบวนการ...

๓) กระบวนการประมวลผลและการใช้ข้อมูล (Process and Use)

(๑) กำหนดให้ทุกชุดข้อมูลต้องระบุสิทธิการสร้าง เข้าถึงเพื่ออ่าน เข้าถึงเพื่อแก้ไข และเข้าถึงเพื่อลบข้อมูล (CRUD : Create – Read – Update – Delete)

(๒) กำหนดให้มีการตรวจสอบและรายงานการเข้าถึงข้อมูลในประเด็นการเข้าถึงที่ผิดนโยบาย หรือ การเข้าถึงที่ผิดปกติที่มีความเสี่ยงต่อการโดนโจมตี และตรวจสอบชั้นความลับของข้อมูลว่าสามารถประมวลผลและใช้ได้หรือไม่ พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ตามบทบาทและภารกิจตามกฎหมายหน่วยงานนั้น ๆ

(๓) กำหนดให้มีการตรวจสอบการเข้าถึงข้อมูลในประเด็นการเข้าถึงที่ผิดนโยบาย หรือ การเข้าถึงที่ผิดปกติที่มีความเสี่ยงต่อการโดนโจมตี และต้องรายงานต่อคณะกรรมการที่เกี่ยวข้อง

(๔) เจ้าของข้อมูลต้องจัดทำสัญญาอนุญาต บันทึกข้อตกลง (Memorandum of Understanding: MOU) สัญญารักษาความลับ (Non-disclosure agreement: NDA) ข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA) หรือข้อตกลงอื่นใดว่าด้วยการเชื่อมโยงข้อมูลขององค์กร หรือข้อตกลงในการนำข้อมูลไปใช้

(๕) กำหนดให้มีการตรวจสอบความสอดคล้องกันของข้อมูลระหว่างหน่วยงานที่เกี่ยวข้อง

(๖) กำหนดให้มีการเก็บบันทึกประวัติการเข้าถึงข้อมูลในทุกกิจกรรม

๔) กระบวนการเปิดเผยและการรักษาความลับข้อมูล (Disclosure and Confidentiality)

(๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติขององค์กรที่ประกาศใช้ในปัจจุบัน ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

(๒) กำหนดให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่สามารถอ่านได้ด้วยเครื่อง (Machine-readable)

(๓) กำหนดให้มีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

(๔) กำหนดให้มีการเปิดเผยคำอธิบายข้อมูลควบคู่กับข้อมูลที่เปิดเผย

(๕) ให้มีการกำหนดผู้รับผิดชอบหลัก ขั้นตอน และวิธีการนำชุดข้อมูลขึ้นเผยแพร่

๕) กระบวนการจัดเก็บข้อมูลถาวร (Achive)

(๑) การจัดเก็บข้อมูลถาวรต้องมีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล และปฏิบัติตามแนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล โดยให้เป็นไปตามบทบัญญัติของกฎหมาย

(๒) ให้กำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมในแต่ละประเภท

(๓) การจัดเก็บถาวร ต้องเป็นการดำเนินการกับข้อมูลที่ไม่มีการลบปรับปรุง หรือแก้ไขอีกต่อไป และสามารถนำกลับมาใช้งานได้ โดยให้เป็นไปตามบทบัญญัติของกฎหมาย

(๔) ต้องมีการกำหนดเครื่องมือและกระบวนการที่จะใช้ในการจัดเก็บข้อมูลถาวร และระยะเวลาในการจัดเก็บข้อมูล

(๕) เจ้าหน้าที่...

(๕) เจ้าหน้าที่ผู้ดำเนินการจัดเก็บข้อมูลถาวร ต้องปรับปรุงคำอธิบายข้อมูลและบัญชีข้อมูลให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยให้เป็นไปตามนโยบายการบริหารจัดการคำอธิบายข้อมูลขององค์กร

(๖) กำหนดให้มีสร้างความรู้ความเข้าใจในการจัดเก็บถาวรแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร

๖) กระบวนการทำลายข้อมูล (Destroy)

(๑) การทำลายข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล และปฏิบัติตามแนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล โดยให้เป็นไปตามบทบัญญัติของกฎหมาย

(๒) การทำลายข้อมูล ต้องเป็นการดำเนินการกับข้อมูลที่ไม่ต้องการนำกลับมาใช้งานอีกต่อไป

(๓) ต้องมีการกำหนดอำนาจอนุมัติ สิทธิ และยืนยันตัวตนในการทำลายข้อมูล

(๔) ให้มีการกำหนดวิธีและแนวทางการทำลายข้อมูล เมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลเกินกว่าระยะเวลาที่กำหนด

(๕) เจ้าหน้าที่ผู้ดำเนินการทำลายข้อมูล ต้องปรับปรุงคำอธิบายข้อมูลและบัญชีข้อมูลให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน โดยให้เป็นไปตามนโยบายการบริหารจัดการคำอธิบายข้อมูลขององค์กร

(๖) กำหนดให้มีสร้างความรู้ความเข้าใจในการทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกองค์กร

๔.๒.๒ นโยบายการบริหารจัดการคำอธิบายข้อมูล (Metadata Management Policy)

๑) ให้มีการกำหนดหลักเกณฑ์และมาตรฐานคำอธิบายข้อมูล

๒) ให้มีการกำหนดกระบวนการจัดทำคำอธิบายข้อมูล

๓) ให้มีการกำหนดการควบคุมดูแลและสอบทานคำอธิบายข้อมูล

๔) ให้มีการกำหนดหน้าที่และความรับผิดชอบให้สอดคล้องกับบทบาทของผู้มีส่วนได้ส่วนเสียกับข้อมูล

๕) ให้มีหน่วยงานหรือผู้รับผิดชอบในการบริหารจัดการคำอธิบายข้อมูล จัดทำ ควบคุมดูแล และสอบทานคำอธิบายข้อมูลให้เป็นปัจจุบัน

๖) ให้มีการกำหนดจัดทำคำอธิบายข้อมูลทั้งในเชิงธุรกิจและเชิงเทคนิคกับทุกชุดข้อมูลที่มีคุณค่าสูง (High Value Datasets) ข้อมูลสำคัญ (Critical Data Element) ข้อมูลหลักและข้อมูลที่ถูกสร้าง จัดเก็บ และนำเข้า ในระบบเทคโนโลยีสารสนเทศอย่างครบถ้วน

๗) ให้กำหนดกระบวนการควบคุม การเข้าถึง การกำหนดสิทธิ การปรับปรุงแก้ไขคำอธิบายข้อมูล เพื่อป้องกันความเสี่ยงหรือข้อผิดพลาดในการปฏิบัติงาน

๘) ให้มีการปรับปรุงทะเบียนรายการคำอธิบายข้อมูลให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการสอบทานอย่างสม่ำเสมอ

๔.๒.๓ นโยบาย...

๔.๒.๓ นโยบายคุณภาพข้อมูล (Data Quality Policy)

๑) ให้มีการกำหนดคุณลักษณะข้อมูลที่มีคุณภาพที่ชัดเจน โดยให้กำหนดในแต่ละมิติของคุณภาพข้อมูลได้แก่ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความทันสมัย (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และความพร้อมใช้ (Availability)

๒) ให้มีการกำหนดเกณฑ์คุณภาพข้อมูล (Data Quality Rule) ที่ครอบคลุมการกำหนดระดับคุณภาพข้อมูล (Data Quality Threshold) ในแต่ละเกณฑ์คุณภาพข้อมูล กระบวนการควบคุมการเปลี่ยนแปลงเกณฑ์คุณภาพข้อมูล

๓) ให้มีการติดตามและประเมินคุณภาพข้อมูลอย่างต่อเนื่อง เพื่อให้สามารถติดตามคุณภาพของชุดข้อมูลที่มีคุณค่าสูง (High Value Datasets) ข้อมูลสำคัญ (Critical Data Element) และข้อมูลหลัก (Master Data) ได้อย่างทันการณ์

๔) ให้มีกระบวนการหรือเครื่องมือแจ้งเตือนไปยังเจ้าของข้อมูลและบริกรข้อมูลเมื่อพบว่าชุดข้อมูลมีคุณภาพต่ำกว่าระดับคุณภาพข้อมูลที่กำหนด

๕) ให้มีการตรวจสอบคุณภาพข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนดอย่างสม่ำเสมอ

๖) ให้มีการปรับปรุงคุณภาพข้อมูล (Resolved Data Quality Issues) โดยมีกระบวนการนำข้อมูลที่ไม่ผ่านเกณฑ์การตรวจสอบคุณภาพมาปรับปรุง

๗) ให้มีการวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause Analysis) เพื่อป้องกันไม่ให้เกิดข้อมูลที่ไม่มีคุณภาพขึ้นอีกในอนาคต

๘) ให้กำหนดกระบวนการควบคุมการปรับปรุงคุณภาพข้อมูลที่รัดกุม เช่น กระบวนการบริหารจัดการการเปลี่ยนแปลงข้อมูล กระบวนการขออนุมัติจากผู้ทำหน้าที่อนุมัติและควบคุมดูแลข้อมูล เป็นต้น

๔.๒.๔ นโยบายการจัดหมวดหมู่และระดับชั้นความลับข้อมูล (Data Categories and Data Classification Policy)

๑) ทุกชุดข้อมูลต้องมีการจัดหมวดหมู่ (Data Category) ดังต่อไปนี้

(๑) ข้อมูลสาธารณะ (Public data) หมายถึง ข้อมูลที่สามารถเปิดเผยได้ประชาชนทั่วไปสามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

(๒) ข้อมูลใช้ภายใน (Internal Use Only) หมายถึง ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในขององค์กรซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในองค์กร เป็นต้น

(๓) ข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคลที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ทั้งทางตรงหรือทางอ้อม ตามมาตรา ๖ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๔) ข้อมูลข่าวสารลับ (Classified Information) หมายถึง ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลขององค์กรที่มีคำสั่งไม่ให้มีการเปิดเผยตามระดับชั้นความลับ

(๕) ข้อมูลความมั่นคง (National Security Information) หมายถึง ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

๒) ทุกชุดข้อมูล...

๒) ทุกชุดข้อมูลต้องมีการกำหนดระดับชั้นความลับข้อมูล (Data Classification Level) ดังต่อไปนี้

ระดับที่ ๑ ชั้นเปิดเผย (Open) หมายถึง ข้อมูลที่ได้รับการเปิดเผยต่อสาธารณะชน ดังนั้นจึงไม่มีข้อจำกัดในการนำมาใช้ประโยชน์และไม่มีมีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานขององค์กร

ระดับที่ ๒ ชั้นเผยแพร่ภายในองค์กร (Private) หมายถึง ข้อมูลที่ไม่ใช่ประเภท ลับ ลับมาก หรือ ลับที่สุด และเป็นข้อมูลเพื่อการใช้งานภายในองค์กรเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลในระดับชั้นนี้ สามารถเข้าถึงได้โดยบุคคลภายในองค์กรได้แก่ กรรมการ ผู้บริหาร บุคลากร และ/หรือตัวแทนขององค์กรเท่านั้น ตามหน้าที่ที่ได้รับมอบหมายและสิทธิในการเข้าถึง

ระดับที่ ๓ ชั้นลับ (Confidential) หมายถึง ข้อมูลที่มีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมการเข้าถึงข้อมูลเฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน และห้ามเผยแพร่ต่อบุคคลภายนอกเว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรโดยคณะกรรมการที่เกี่ยวข้อง หรือหน่วยงานที่เป็นเจ้าของข้อมูลขึ้นไป โดยต้องมีการลงนามในเอกสารสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) หรือข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement) เว้นแต่การเผยแพร่ดังกล่าวเป็นไปตามอำนาจที่กฎหมายให้การรับรอง

ระดับที่ ๔ ชั้นลับมาก (Secret) หมายถึง ข้อมูลที่มีความสำคัญต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดโดยจำกัดการเข้าถึงข้อมูลเฉพาะผู้มีอำนาจตามที่กำหนดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการปฏิบัติงาน ซึ่งอาจเป็นกลุ่มคนในหน่วยงานที่เกี่ยวข้องเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลที่ไม่เกี่ยวข้อง

ระดับที่ ๕ ชั้นลับที่สุด (Top Secret) หมายถึง ข้อมูลที่มีความสำคัญสูงต่อการดำเนินงานตามภารกิจขององค์กร โดยต้องได้รับการควบคุมอย่างเข้มงวดที่สุดโดยต้องจำกัดผู้มีอำนาจในการเข้าถึงข้อมูลให้น้อยที่สุดในระดับบุคคลและตำแหน่งงานเท่านั้น เพื่อป้องกันการรั่วไหลไปสู่บุคคลภายนอก และ/หรือ บุคคลที่ไม่เกี่ยวข้อง

๓) การจัดหมวดหมู่และระดับชั้นความลับข้อมูลต้องดำเนินการโดยบริกรข้อมูลและเจ้าของข้อมูลร่วมกัน โดยต้องมีการบันทึกหรือระบุชั้นความลับของชุดข้อมูลในแต่ละชุดข้อมูลในระบบที่จัดเก็บคำอธิบายข้อมูลของชุดข้อมูลตามที่องค์กรกำหนดไว้

๔) การกำหนดสิทธิของบุคคลหรือคณะบุคคลในการเข้าถึงชุดข้อมูลให้ดำเนินการโดยบริกรข้อมูลหรือผู้ที่ได้รับมอบหมายร่วมกับเจ้าของข้อมูล และต้องกำหนดให้สอดคล้องกับชั้นความลับข้อมูลขององค์กร

๕) ข้อมูลที่มีระดับชั้นความลับระดับที่ ๓ เป็นต้นไป จะต้องมีกระบวนการในการร้องขอข้อมูลและต้องมีการบันทึกข้อมูลที่เกี่ยวข้องกับการร้องขอที่สามารถตรวจสอบความถูกต้องย้อนหลังได้

๖) ให้มีการทบทวนหมวดหมู่และระดับชั้นความลับข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๔.๒.๕ นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Exchange Policy)

๑) ให้กำหนดกระบวนการในการร้องขอ แลกเปลี่ยน และเชื่อมโยงให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนการดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

๒) ให้กำหนดคำอธิบายข้อมูลของชุดข้อมูลที่มีการร้องขอ แลกเปลี่ยนและเชื่อมโยงให้ครบถ้วน

๓) ทำสัญญาอนุญาตบันทึกข้อตกลง (MOU) สัญญาการรักษาข้อมูลที่เป็นความลับ (NDA) ข้อตกลงการแบ่งปันข้อมูล (DSA) หรือข้อตกลงอื่นใดว่าด้วยการเชื่อมโยงข้อมูลของ กปน. หรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

๔) ให้กำหนดเทคโนโลยี มาตรฐานทางเทคนิค และความมั่นคงปลอดภัยที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูล ให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง

๕) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการร้องขอ แลกเปลี่ยนและเชื่อมโยงข้อมูล (Log Files) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖) สามารถตรวจสอบได้ว่าการร้องขอ แลกเปลี่ยนและเชื่อมโยงข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการร้องขอ แลกเปลี่ยนและเชื่อมโยงข้อมูล

๗) ตรวจสอบชั้นความลับข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ เช่น ไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับของทางราชการ และความเป็นส่วนบุคคล เป็นต้น พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ

๔.๒.๖ นโยบายการเปิดเผยข้อมูล (Open Data Policy)

๑) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หลักเกณฑ์ นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดก็ตาม

๒) ต้องได้รับการอนุญาตจากเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

๓) ให้มีการกำหนดผู้รับผิดชอบ ขั้นตอน และวิธีการนำชุดข้อมูลขึ้นเผยแพร่สู่สาธารณะ

๔) ให้มีการคัดเลือกชุดข้อมูลเปิดที่จะนำไปเผยแพร่บนศูนย์กลางข้อมูลเปิดภาครัฐ

๕) การเปิดเผยข้อมูลต้องมีการจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่กำหนด

๖) ให้มีการเปิดเผยคำอธิบายข้อมูลของชุดข้อมูลเปิด

๗) มีการตรวจสอบว่าการเปิดเผยชุดข้อมูลเปิดได้ถูกดำเนินการตามแนวทางและขั้นตอนที่ได้กำหนดไว้

๔.๒.๗ นโยบายความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูล (Data Security and Privacy Policy)

๑) กำหนดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ของการประปานครหลวง

๒) กำหนดให้มีการรักษาความเป็นส่วนตัวของข้อมูล ตามประกาศการประปานครหลวง เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๕ ให้มีการดำเนินการตรวจสอบ ทบทวนและปรับปรุงนโยบายอย่างต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ นโยบาย...

ข้อ ๖ นโยบายตามข้อ ๔ ถือเป็นมาตรฐานด้านธรรมาภิบาลข้อมูลขององค์กร โดยให้ดำเนินการอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “แนวปฏิบัติการดำเนินการธรรมาภิบาลข้อมูล” เพื่อใช้เป็นแนวทางในการบริหารจัดการข้อมูลให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีความมั่นคงปลอดภัย มีการรักษาความเป็นส่วนบุคคล มีความเชื่อมโยงและเป็นประโยชน์ต่อไป

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่๑๓ กันยายน พ.ศ. ๒๕๖๗

(นายรักษ์ศักดิ์ สุริยหาร)
รองผู้ว่าการ (วิศวกรรม) รักษาการในตำแหน่ง
ผู้ว่าการการประปานครหลวง

ที่ กกล.ว ๑๘๔/๒๕๖๗
เรียน หน่วยงานต่าง ๆ
เพื่อโปรดทราบ

๑๖ ก.ย.๖๗
(น.ส.นวลจันทร์ เทียมสมัย)
ผู้อำนวยการกองกลาง